TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

NÁVRH OBCHODNÍHO MODELU POSKYTUJÍCÍHO SLUŽBY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Bakalářská práce

Studijní program: B6209 – Systémové inženýrství a informatika
Studijní obor: 6209R021 – Manažerská informatika

Autor práce: **Michal Hager**
Vedoucí práce: Ing. Zbyněk Hubínka

Liberec 2014

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Economics

DESIGN OF BUSINESS MODEL PROVIDING SERVICES IN THE FIELD OF CYBER SECURITY

Bachelor thesis

Study programme: B6209 – System Engineering and Informatics
Study branch: 6209R021 – Managerial Informatics

Author: **Michal Hager**
Supervisor: Ing. Zbyněk Hubínka

Liberec 2014

Tento list nahraďte
originálem zadání.

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Poděkování

Tímto bych chtěl poděkovat vedoucímu mé bakalářské práce Ing. Zbyňku Hubínkovi za odborné vedení a kvalifikované rady a připomínky, které mi pomohly při tvorbě bakalářské práce. Stejně tak bych rád poděkoval všem, u kterých jsem hledal a našel pomoc a rady. Velké děkuji patří také konzultantovi mé bakalářské práce Janu Chudanovi.

Anotace

Bakalářská práce se zabývá především tématem kybernetické bezpečnosti. Výsledkem této práce je návrh obchodního modelu, který by poskytoval služby v oblasti kybernetické bezpečnosti. Práce je rozdělena do dvou částí, a sice část teoretickou a část praktickou. Teoretická část se věnuje především definici pojmu kybernetické bezpečnosti, analýze současného stavu kybernetické bezpečnosti v České republice a rozebírá nový návrh zákona o kybernetické bezpečnosti z hlediska možnosti poskytování bezpečnostních služeb. Na ni navazuje část praktická, ve které byly použity poznatky získané z teoretické části. Zaobírá se návrhem obchodního modelu, jeho následnému vyhodnocení a popisuje možnosti dalšího rozvoje.

KLÍČOVÁ SLOVA: Kybernetická bezpečnost, obchodní model, návrh zákona o kybernetické bezpečnosti.

Anotation

This thesis mainly deals with the topic of cyber security. The result of this work is a design of a business model that would provide services in the field of cyber security. The work is divided into two parts, namely the theoretical part and the practical part. The theoretical part is devoted mostly to definition of the concept of cyber security, the analysis of the current state of cyber security in the Czech Republic and discusses the new bill about cyber security from the viewpoint of providing security services. It is followed by the practical part, which used the knowledge gained from the theoretical section. It deals with the design of the business model, its subsequent evaluation and describes the possibilities of further development.

KEY WORDS: Cyber security, business model, bill about cyber security.

Obsah

Seznam obrázků a tabulek

Seznam obrázků

Seznam tabulek

Seznam zkratek

ALE	Annual Loss Expentancy
BSI	British Standards Institution
CC	Common Criteria
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
ČVÚT	České Vysoké Učení Technické
EMEA	Europe, the Middle East and Africa
ENISA	European Union Agency for Network and Information Security
EZÚ	Elektrotechnický Zkušební Ústav
FIRST	Forum of Incident Response and Security Teams
IBM	International Business Machines
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention Systems
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
NBÚ	Národní Bezpečnostní Úřad
PDCA	Plan – Do – Control – Act
TCSEC	Trusted Computer System Evaluation Criteria
TERENA	Trans-European Research and Education Networking Association
VBS	Visual Basic Script
VPN	Virtual Private Network
VÚPS	Výzkumný Ústav Pozemních Staveb

Úvod

V posledních letech jsme svědky obrovského pokroku a rozvoje v užívání informačních a komunikačních technologií. Ty pronikly do reality a každodenního fungování současné společnosti, a to zejména internet a mobilní telefony. Většina naší komunikace se děje v tzv. kybernetickém prostoru právě jejich prostřednictvím. Informace jsou považovány za hlavní zdroj ekonomického, sociálního a kulturního pokroku. Na trhu se začaly objevovat tzv. „chytré“ spotřebiče (např. ledničky). Hovoříme o tzv. informační explozi a postupně se již ustálil pojem informační společnost. Měřítkem úrovně informační společnosti není úroveň hardwaru, ale rozsah, kvalita, relevance a dostupnost informací a informačních služeb.

Narůstající užití informačních a komunikačních technologií v činnostech organizací, firem i jednotlivců pak vyžaduje, aby při zpracování, přenosu, ukládání a opětovném využití objemů dat nedocházelo ke ztrátě životně důležitých údajů, ke vzniku chyb, kompromitaci nebo neoprávněné modifikaci dat. To vše a mnohem více má za úkol infromační bezpečnost. Je potřeba zavádět v organizaci řízení a řešení informační bezpečnosti s příslušným odborným personálním obsazením v podobě bezpečnostního managementu.

Cílem této práce je navrhnout obchodní model, který by poskytoval služby právě v oblasti informační bezpečnosti. Na cestě k tomuto cíli je potřeba nejdříve proniknout do problematiky informační bezpečnosti. Proto se práce v první části věnuje například definici kybernetického prostoru, bezpečnostním hrozbám a rizikům, útokům a útočníkům na informační bezpečnost, vztahu managementu a informační bezpečnosti a normám, které s ní souvisí. Protože se jedná o návrh modelu, který má najít uplatnění v současné době, jsou v práci uvedeny aktuální statistiky nahlášených incidentů. Tuto oblast bude ovlivňovat nový zákon o kybernetické bezpečnosti, který by měl nabýt platnosti k 1.1.2015, a proto se práce věnuje jeho návrhu v druhé fázi teoretické části, a to zejména z hlediska možnosti poskytování bezpečnostních služeb.

1 Literární rešerše v oblasti kybernetické bezpečnosti

Při hledání v databázích ProQuest jsem našel hned několik užitečných článků. Článek s názvem *„Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications“*[1] se zaměřuje na hrozby v oblasti kybernetické bezpečnosti. Autoři poukazují na to, že s exponenciálním nárůstem používání kyberprostoru, roste exponenciálně také kybernetická kriminalita. Všímají si také, že tím, jak se webové aplikace stávají stále více komplexnějšími a složitějšími, se zvyšuje počet konstrukčních vad (uvádí, že až 90% webových aplikací má nějakou konstrukční vadu), což umožňuje zneužití kybernetickými zločinci. Jádrem článku je detailní analýza existujících systémů a metodik pro řešení kybernetické bezpečnosti.

Článek *„Optimizing investments in cyber-security for critical infrastructure“*[2] se věnuje optimalizaci investic do kybernetické bezpečnosti v kritické infrastruktuře. Autoři zmiňují, že tyto investice musí vyrovnávat úspory, které vzniknou při předcházení narušení, detekci kybernetických útoků a zmírnění fyzických škod způsobených útočníkem na počítačem ovládané zařízení. Autoři v článku nastiňují metodu pro optimalizaci těchto investic. Metoda definuje bezpečnostní funkce přinášející největší ochranu při fixním rozpočtu.

Další článek s názvem *„Cyber-risk decision models: To insure IT or not?“*[3] navrhuje

---

[1] Masood, M. – Hur, A. – Razzaq, A. – Ahmad, H. F. *Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications*, IEEE Eleventh International Symposium on Autonomous Decentralized Systems, 2013, s. 1-5. ISBN: 978-1-4673-5069-3. Dostupné také z WWW: http://www.computer.org/csdl/proceedings/isads/2013/5069/00/06513420-abs.html.

[2] Patterson, I – Nutaro, J. – Allgood, G. – Kuruganti, T. – Fugate, D. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop.* Článek č. 20, ACM, New York, NY, USA, 2013, s. 1-4. ISBN: 978-1-4503-1687-3. Dostupné také z WWW: http://dl.acm.org/citation.cfm?doid=2459976.2459999.

[3] Mukhopadhyay, A. – Chatterjee, S. – Saha, D. – Mahanti, A. – Sadhukhan, S. K. *Decision Support Systems.* Svazek 56, Elsevier science BV, Amsterdam, Nizozemsko, 2013, s11-26. ISSN**:** 0167-9236. Dostupné také z WWW: http://www.sciencedirect.com/science/article/pii/S0167923613001115.

modely pro pomoc firmám při rozhodování, jaký produkt pro zajištění kybernetické bezpečnosti zvolit a v jakém rozsahu jej mohou použít. Autoři navrhují pro posouzení zranitelností a výpočet očekáváných ztrát zvolit model Copula-aided Bayesian Belief Network (CBBN).

Co se týče knižní literatury, byla pro mě největším přínosem publikace *„Vybrané aspekty informační bezpečnosti“*[4] věnující se pojmům informační bezpečnosti, bezpečnostním hrozbám a rizikům, kybernetické kriminalitě a ochraně dat. Publikace poskytuje velmi dobře zpracovaný teoretický základ.

Z dalších děl věnujících se tématu lze uvést publikaci *„Řízení bezpečnosti informací“*[5], která poskytuje přesnou definici pojmu informační bezpečnost a poskytuje přehled metod pro hodnocení a řízení informační bezpečnosti. Publikace *Počítačová bezpečnost a ochrana dat*[6] výstižným způsobem popisuje ochranu spravovaných či přenášených dat před ztrátou, zmizením, zcizením či zneužitím. Řeší předcházení bezpečnostním incidentům, ať už se jedná o útok hackera, virovou hrozbu nebo zneužití dat zaměstnanci. Nalezneme v ní také informace o problematice elektronického a digitálního podpisu, fyzickém zabezpečení dat, bezpečnostní politice firmy či šifrování a autentizaci.

Nelze zapomenout ani na publikaci *„Krizový management. Krizová komunikace“*[7], která poskytuje zejména podrobný popis způsobů, jak zvládat komunikaci před krizí, v době krize a postkrizovou komunikaci. K řešeným problémům uvádí příklady, jak by měla komunikace v takovém případě vypadat.

---

[4] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, ISBN 978-80-7251-339-0.

[5] Douček, P. – Novák, L. – Svatá, V. – Nedomová, L. *Řízení bezpečnosti informací*. 1. vyd. Professional Publishing, 2008, ISBN 978-80-86946-88-7.

[6] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vyd. Brno: Computer Press, 2004, ISBN 80-251-0106-1.

[7] Antušák, E. – Kopecký, Z. *Krizový management. Krizová komunikace.* 1. vyd. Vysoká škola ekonomická v Praze, Oeconomica, 2005, s. 25-70, ISBN 80-245-0945-8.

2 Kybernetická bezpečnost

2.1 Pojem informační bezpečnost

"Bezpečnost informací (Information Security) – zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost, hodnověrnost." [8]

Informační bezpečnost je v současné době velmi frekventovaný pojem a jeho důležitost má vzestupnou tendenci. Tuto tendenci má především z důvodu rostoucí hodnoty informací v oblasti soukromého podnikání i státní správy. Informace mají různou podobu. Od elektronické přes tištěnou až například po informace, které lze vypozorovat z logistických procesů nebo rozmístění jednotlivých pracovišť. Rizika úniku a zneužití informací hrozí zejména zevnitř organizace. Většina nezabezpečených míst není zřejmá, o to užitečnější jsou pak rady profesionálů s bohatými zkušenostmi. Informační bezpečnost je komplexní pohled, který organizaci pomáhá poznat a také chránit své cenné informace. Pomocí praktických opatření vede k elimininaci či výraznému snížení dopadů v případě, že nastane mimořádná událost.

Pro účinnou ochranu je důležité pochopit, jaké informace organizace má a jakou hodnotu pro ni znamenají. Je také zásadní uvědomit si cíle a reálné fungování organizace. Jen tak lze navrhnout opravdu účinný a efektivní systém řízení informační bezpečnosti. Cílem není pouhé zavedení systému řízení informační bezpečnosti, ale i jeho dlouhodobá funkčnost a rozvoj. Měl by být schopen reagovat na změny organizace i jejího okolí. Zavedením funkčního systému řízení informační bezpečnosti lze v organizaci minimalizovat rizika spojená s únikem informací. Napomáhá také snížení nákladů ICT a celkově přispívá k efektivitě procesů. Znamená výraznou oporu v rozhodovacích procesech na úrovni managementu ICT i na úrovni vrcholového managementu.

[8] Douček, P. – Novák, L. – Svatá, V. – Nedomová, L. *Řízení bezpečnosti informací*. 1. vyd. Professional Publishing, 2008, s. 59, ISBN 978-80-86946-88-7.

K hlavním důvodům pro implementaci informační bezpečnosti organizace patří:

- vzájemné prorůstání a vzájemné ovlivňování ekonomik a dalších odvětví hospodářství prostřednictvím informačních a komunikačních technologií,
- doba, kdy je stále více dat předáváno v digitální formě, citlivá data z pohledu celé společnosti jsou uložena v informačních systémech a v případě jejich výpadku či ztráty by byla ohrožena akceschopnost infrastruktur,
- způsoby a techniky přenosu dat v sítích jsou z drtivé většiny všeobecně známé ve formách přenosových a komunikačních standardů, což vede k ohrožení dat útočníky.

Všechny státní organizace, počítačové firmy i soukromé podniky musí nejen budovat informační bezpečnost, ale také ji neustále inovovat. Podle výzkumů jsou lidé nejrizikovějším faktorem kompromitace, modifikace, vyzrazení, úniku a zničení citlivých dat a informací v organizaci. Informační bezpečnost má jistě zásadní význam pro ty instituce, které ji prodávají jako součást své produkce. Softwarové, právnické a konzultační firmy ji dokonce prodávají jako jejich hlavní komoditu. Závada v technické dokumentaci, dohromady s lidským selháním a technickou závadou, se řadí ke třem hlavním příčinám nežádoucích provozních událostí v jaderném průmyslu a letectví.

2.2 Kybernetický prostor [9]

Výraz kyberprostor je uměle vytvořeným slovem. Poprvé ho použil W. Gibson v roce 1984 ve své knize Neuromancer, přičemž vycházel ze základů kybernetiky jako vědního oboru. Kybernetika je věda zabývající se systémy komunikace a řízení v živých systémech, organizacích a také strojích. Kybernetickým prostorem chápeme virtuální svět vytvořený moderními informačními a komunikačními prostředky, paralelně ke světu reálnému.

[9] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti.* 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 13, ISBN 978-80-7251-339-0.

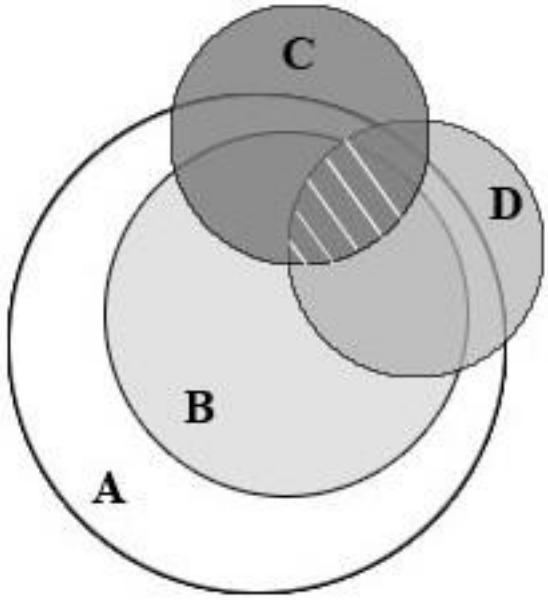
Výměna dat mezi počítačovými sítěmi a servery tak lze popsat jako procházku kyberprostorem.

V tomto virtuálním světě nezná lidská fantazie hranice. Je prostorem pro experimenty. Projektují, plánují, realizují a analyzují se tu jevy a procesy v prostředí blízkém životu, často předtím než proběhnou ve skutečné realitě. Umožňuje lidem spolu komunikovat, reagovat a užívat fantazii mimo hranice času, prostoru, jazyka i kultury. Ve srovnání s virtuálním světem multimédií zde přibývá ještě možnost interakce s dějem a jinými lidmi. To umožňuje další vývoj společenských fantazií a projektů a zároveň zdokonaluje virtuální svět.

2.3 Vztah managementu a informační bezpečnosti [10]

Pro znázornění vzájemných vztahů mezi managementem a informační bezpečností nejlépe poslouží Vennův diagram v množinovém vyjádření. Bezpečnostní managament je podmnožinou managementu, ten se dělí na další podobory, které ale není potřeba detailně popisovat. Prvky informační bezpečnosti "D" se týkají bezpečnosti dat a informací, a to v jakékoli formě. Proto se prvky informační bezpečnosti "D" stýkají s prvky ze všech ostatních oblastí. Průnik všech čtyř množin, na obrázku vyznačen šrafovanou oblastí, znázorňuje oblast bezpečnostního managementu informační bezpečnosti a informatiky. Z diagramu lze také vyvodit to, že vzájemné vztahy či vazby jednotlivých vědních disciplín se ovlivňují a prolínají.

[10] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 14-15, ISBN 978-80-7251-339-0



A – Management

B – Bezpečnostní management

C – Informatika

D – Informační bezpečnost

Obrázek 1: Vennův diagram zobrazující vztah 4 množin vyskytujících se ve firemní struktuře
Kalamár, Š. – Požár, J. Vybrané aspekty informační bezpečnosti. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 14, ISBN 978-80-7251-339-0.

2.4 Bezpečnostní hrozby a rizika

Hrozba způsobuje nežádoucí incident, jež má často za následek poškození informačního systému nebo organizace a jejich aktiv. Hrozby jsou přírodní podstaty, mohou ale hrozit také vlastní zaměstatnanci nebo vnější útočník. Hrozby jsou náhodné, nebo úmyslné. Škoda napáchaná incidentem může být dočasné nebo trvalé povahy. To, že některé vlivy prostředí, ve kterém se informační systém provozuje, způsobují hrozby, se děje díky zranitelným místům informačního systému. Pojmem hrozba značíme okolnost či událost působící na zranitelné místo aktiva, jež může způsobit potenciální škodu. Hrozba je skutečnost možného ohrožení, kdy se zatím nic nestalo, ale stát se může. Až tato událost nastane, pak hovoříme o bezpečnostním incidentu.

2.4.1 Druhy hrozeb v informační bezpečnosti [11]

Hrozby se dělí podle hledisek především na:

- objektivní
  - přírodní či fyzické (požár, povodeň, výpadek napětí, poruchy). Zde je prevence obtížná, potřeba vypracování vhodného havarijního plánu,
  - fyzikální (elektromagnetické vyzařování),
  - technické či logické (porucha paměti, softwarová "zadní vrátka", špatné propojení jinak bezpečných komponent apod.),
- subjektivní
  - neúmyslné (působení neškoleného uživatele nebo správce informačního systému),
  - úmyslné (teroristé, konkurenti, hackeři, vnitřní útočníci).

Dá se říci, že příklady uvedené v závorkách se dají charakterizovat také jako zdroje ohrožení. K současným hrozbám patří zejména neautorizovaná modifikace informací, informačních zdrojů a služeb, orientační přehled hrozeb pro distibuované systémy informačních technologií, neautorizované zpřístupnění informací odposlechem na přenosovém médiu, neoprávněné kopírování z dočasných paměťových míst.

Při zaměření na hrozby v informačních systémech se jedná především o:

- přerušení (určitá část systému je ztracena nebo nedosažitelná),
- zachycení (neautorizovaný subjekt získá přístup k objektu systému a útočník tak může zachytit a získat citlivé informace),
- modifikace (neautorizovaný subjekt, útočník úmyslně modifikuje data a informace či celé části systému),
- fabrikace (neautorizované vytvoření nového klamného objektu, díky kterému může útočník provádět nekontrolované akce, které narušují informační bezpečnost počítačového systému).

[11] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 20-22, ISBN 978-80-7251-339-0.

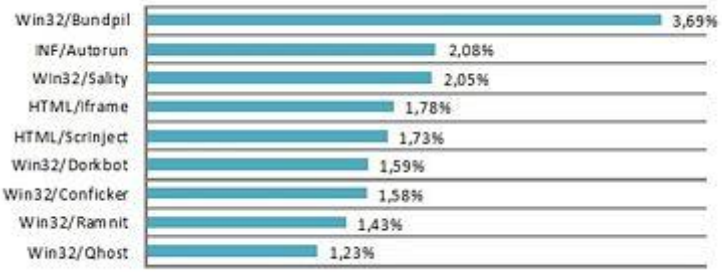
Současně s hrozbami je nezbytné uvést také související místa zranitelnosti počítačových systémů. Rozlišujeme tři hlavní místa zranitelnosti:

- utajení - určité objekty v počítačovém systému mohou být přístupné pouze přesně vymezeným autorizovaným subjektům,
- integrita - vymezené objekty mohou být modifikovány pouze oprávněnými subjekty,
- dosažitelnost - určité objekty jsou dostupné pro autorizované subjekty a uživatele.

2.4.2 Nejrozšířenější internetové hrozby [12]

Podle nedávno provedené analýzy společnosti Eset (září 2013) zažívají v posledních měsících největší rozmach počítačové hrozby, které se šíří prostřednictvím vyměnitelných médií (USB flash disky, externí pevné disky, CD i DVD nosiče).

V současnosti nejrozšířenější hrozbou ve světě je červ Win32/Bundpil (3,69 %). Jde o červa šířícího se pomocí přenosných médií.

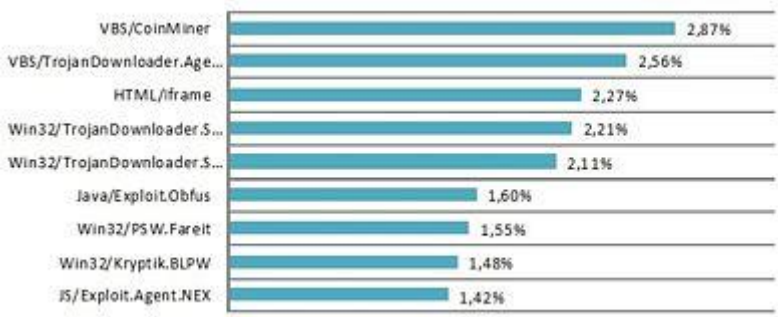


Obrázek 2: Nejrozšířenější hrozby ve světě

Novinky [online]. 2013. Dostupné z WWW:
http://www.novinky.cz/internet-a-pc/316722-nejrozsirenejsi-internetove-hrozby.html.

[12] Novinky [online]. 2013. Dostupné z WWW:
http://www.novinky.cz/internet-a-pc/316722-nejrozsirenejsi-internetove-hrozby.html.

V České republice je v současnosti nejrozšířenější hrozbou trojský kůň VBS/CoinMiner (2,87 %).



Obrázek 3: Nejrozšířenější hrozby v České republice

Novinky [online]. 2013. Dostupné z WWW: http://www.novinky.cz/internet-a-pc/316722-nejrozsirenejsi-internetove-hrozby.html.

2.4.3 Riziko [13]

Riziko se zjišťuje v procesu nazývajícím se analýza rizik. Ta spočívá v odhalení a definici všech možných hrozeb a v určení pravděpodobnosti, že určitá hrozba bude prostřednictvím slabin uskutečněna. Výsledkem je především souhrn doporučených protiopatření, která snížují riziko na minimum. Nepodchycené riziko se nazývá zbytkové riziko. Je to riziko, které přijímáme, protože může způsobit malé škody nebo se objevuje v dlouhých intervalech.

Počítá se tzv. ALE, tedy očekávaná roční ztráta.

(1)

$$\mathrm{ALE} = \sum_{i=1}^{n} p_i * c_i ,$$

kde *p* je pravděpodobnost, že během jednoho roku nastane ohrožení; *c* je ztráta, jestliže k ohrožení dojde; *i* je pořadí ohrožení; *n* je celkový počet ohrožení za rok. Je nutné zjistit,

[13] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 24, ISBN 978-80-7251-339-0.

zda náklady na protiopatření pro ochranu aktiv nepřesahují výši možných škod. U ochrany informací hraje důležitou roli právě i její cena. Nejlepší je tedy dosáhnout takové úrovně zabezpečení, kde se vynaložené náklady rovnají případné ztrátě.

2.5 Bezpečnostní incidenty a jejich minimalizace

Za bezpečnostní incident považujeme poškození či ztrátu datových souborů, delší vyřazení systému z provozu, rozšíření počítačových virů v síti nebo průnik do informačního systému.

2.5.1 Postup pro řešení bezpečnostních incidentů [14]

Postup pro řešení incidentu by měl vypadat následovně:

1. zjistit zdroj,
2. zajistit důkazy podrobným šetřením,
3. zjistit možnosti fyzického přístupu ke zdroji a osobní odpovědnost pracovníků,
4. zpracovat protokol s osobami, které byly, mohly být či neměly být účastníky incidentu,
5. po prošetření vyvodit disciplinární nebo kázeňská opatření s viníky,
6. přijmout technická režimová a další preventivní opatření v informačním systému a na příslušných pracovištích.

[14] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 26-29, ISBN 978-80-7251-339-0.

2.5.2 Prevence bezpečnostních incidentů [15]

Předejít zneužití, poškození, zcizení nebo zničení informací lze díky analýze dosavadních i předpokládaných příčin a podmínek zločinnosti v oblasti práce s informacemi. Z hlediska rozsahu působení prevence je možné ji dělit na:

- obecnou
  - opatření působí bez ohledu na to, zda nebezpečí již vzniklo, působí na všechny objekty a subjekty užívání a zpracování informace. Jedná se např. o právní vzdělání, výchovu k vysoké profesionalitě, výchovu k solidaritě s oborem činnosti a podnikem, výchovu k bdělosti, správnou personální práci apod.,
- zvláštní (individuální)
  - opatření zaměřeno na vybrané jevy, procesy a řízení, např. technické procesy, přenosové kanály, konfliktní jedinci apod.,
- situační prevenci
  - realizace rychlých operativních opatření, která vyplynou ze situace. Cílem opatření je zabránit, odvrátit a překazit vznik dalších škod nebo zmírnit následky působení určitých příčin a podmínek.

2.5.3 Krizová komunikace [16]

Jedním z důležitých nástrojů pro úspěšné zvládnutí bezpečnostních incidentů (a následné krize) je krizová komunikace. Z odborného hlediska je krizová komunikace specifická forma sociální komunikace a současně je nástrojem krizového managementu. Může mít formu verbální a neverbální. Charakterově se jedná především o interpersonální, jedno i dvousměrnou, veřejnou, meziosobní, skupinovou a masovou komunikaci.

---

[15] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 29-30, ISBN 978-80-7251-339-0.

[16] Antušák, E. – Kopecký, Z. *Krizový management. Krizová komunikace.* 1. vyd. Vysoká škola ekonomická v Praze, Oeconomica, 2005, s. 25-70, ISBN 80-245-0945-8.

S krizemi je potřeba počítat, předvídat je, připravit se na ně. Součástí této přípravy je i připravenost vést krizovou komunikaci. Nejedná se tedy pouze o komunikování v době krize (po incidentu), ale také před incidentem. Cílem je uvolnit správné (včasné, hodnotné, důvěryhodné a přesvědčivé) informace ve správný čas a na správném místě. Pro dosažení tohoto cíle je nutné držet se základních principů a pravidel úspěšné krizové komunikace, např.:

- princip přímé odpovědnosti,
- princip přesnosti a stručnosti,
- princip očekávané reakce,
- nedopustit, aby kritika (zejména tisku) zůstala bez odpovědi,
- mít připravený scénář krizové komunikace a mít stanovené role,
- pravidelně aktualizovat krizový plán,
- a mnohé další.

Každá krize se rozprostírá do několika dimenzí (dimenze provozní činnosti, managementu oběti, chování, etiky, ponaučení atd.) a jestliže kterákoli z nich není dostatečně ovládána, může to narušit či zničit řešení situace, obnovu a navrácení systému do původního stavu. Schéma, které ukazuje správný průběh procesu vytvoření a implementování modelu krizové komunikace, tvoří přílohu D.

2.6 Útoky a útočníci na data a informace

Ukazuje se, že při únicích nebo zneužití informací je nejslabším článkem v celém systému ochrany lidský faktor. Nejrizikovějším faktorem úniku informací jsou právě vlastní, interní zaměstnanci organizace (až 80% případů). Nejčastěji se tento jev vyskytuje na pracovištích marketingu či reklamního oddělení. Konkurence zde má zájem získat podrobnosti o zásobování surovinami, o vlastních odběratelsko-dodavatelských vztazích, síti obchodních zástupců apod. Často také otázky kladené kupujícími mohou být zaměřeny na získávání informací pro konkurenci.

Ochrana CD, DVD, disket a jiných médií obsahujících cenné informace, je značně podceňována. A to nejen z hlediska důvěrnosti či integrity, ale i z hlediska dostupnosti.

2.6.1 Klasifikace útočníků [17]

Útočníci mají různé znalosti a vybavenost. Obecně útočníkem může být jak amatér, tak i hacker či profesionální zločinec. Právě síla (vybavenost) útočníka se zohledňuje při volbě protiopatření a jeho síly. Uvádí se tři základní druhy útočníků:

- vnitřní útočník
  - osoba s připojením do vnitřní komunikační sítě organizace,
  - možná obrana jednak zvyšováním loajality k zaměstnavateli nebo zvyšováním spolehlivosti,
- vnější útočník
  - osoba, která nemá fyzický přístup k vnitřní komunikační síti,
  - jedinou obranou je důkladné zabezpečení systému,
- celý svět (internet)
  - jedná se o nejnebezpečnějšího útočníka,
  - neexistuje žádná opravdu účinná ochrana.

2.6.2 Charakteristika útoků na data a informace [18]

Útokem rozumíme úmyslné využití zranitelného místa, které má za cíl škodu na aktivech, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Možné formy útoků jsou:

[17] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 35-37, ISBN 978-80-7251-339-0.

[18] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 37-43, ISBN 978-80-7251-339-0.

- přerušením
  - aktivní útok na dostupnost,
  - např. ztráta, znepřístupnění, poškození aktiva,
- odposlechem
  - pasivní útok na důvěrnost,
  - např. okopírování dat,
- změnou
  - aktivní útok na integritu,
  - např. změna uložených nebo přenášených dat,
- přidáním hodnoty
  - aktivní útok na integritu nebo útok na autenticitu,
  - např. podvržení transakce, dodání falešných dat.

Místem nejčastějších útoků na operační systém je jeho mechanismus zpracování vstupně-výstupních operací. Zařízení, která realizují vystupně-výstupní operace, jsou totiž do značné míry samostatná a na zbytku systému nezávislá. Mezi možné útoky lze zahrnout:

- zadní vrátka - skrytý softwarový nebo hardwarový mechanismus, který může útočník využít k porušení bezpečnosti informačního systému,
- trojský kůň - program vykonávající kromě obvyklých funkcí ještě další skryté akce, které se aktivují po splnění jisté podmínky,
- salámový útok - technika podvodu, kdy při velkém množství finančních transakcí může celkově vznikout velká finanční škoda,
- skryté kanály - chtějí-li programátoři získat přístup ke zpravovaným informacím, vytvoří skrytý kanál, aby měli přístup k běžícím programům i po ukončení vývoje,
- hladové programy - programy, které pro svou činnost vyžadují velkou část výkonu systému,
- červi - síťová obdoba počítačových virů šířící se prostřednictvím komunikačních linek.

2.7 Normy informační bezpečnosti [19]

Významným krokem k tomu, aby situace v informační bezpečnosti vypadala tak, jak vypadá dnes, bylo vydání harmonizovaných kritérií Evropských společenství pod názvem „*Kritéria hodnocení bezpečnosti informačních systémů*“, známých pod zkratnou ITSEC.

Kritéria ITSEC vymezují sedm tříd míry zaručitelnosti bezpečnosti IT (E0 až E6) a v příloze definují dalších deset tříd bezpečnostní funkčnosti (F-xx). Ty slouží pouze jako příklady a pro usnadnění práce uživatelům kritérií. Uživatel má tedy možnost vytvořit sám vlastní třídu bezpečnostní funkčnosti, která je ovšem v souladu s požadavky kritérií ITSEC.

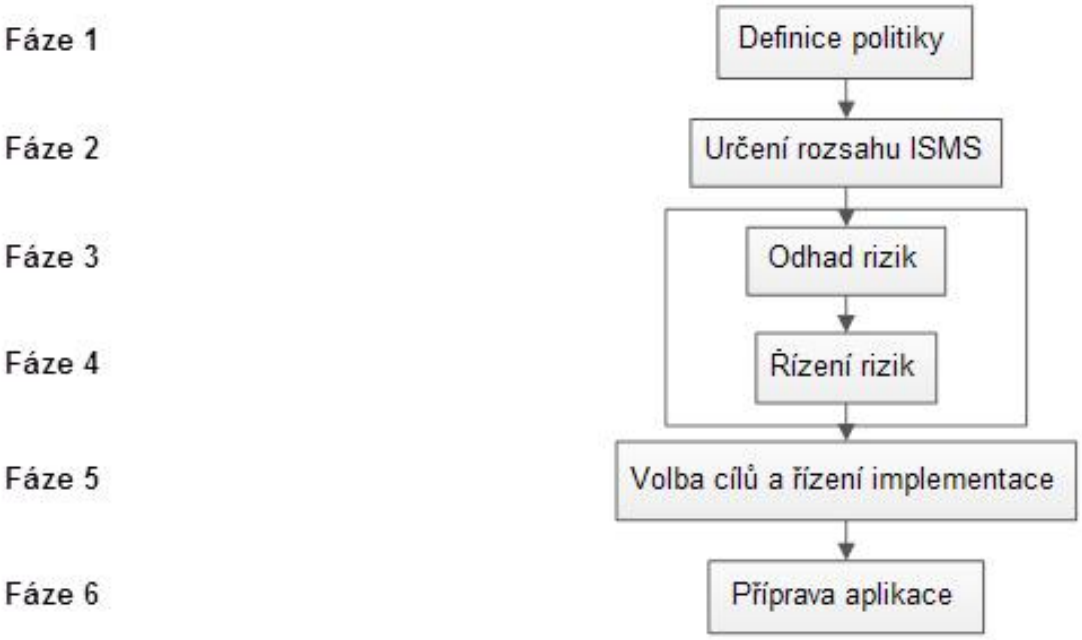
V současnosti se jedná především o společná kritéria (norma ISO/IEC 15408) a rodinu norem ISO/IEC 27000. Společná kritéria vznikla ze tří již existujících standardů: ITSEC, CTCPEC a TCSEC. Společná kritéria dávají jistotu, že se proces specifikace, implementace a hodnocení produktu počítačové bezpečnosti bude řídit přísným a standardizovaným způsobem. Rodina norem ISO/IEC 27000 se věnuje především řízení bezpečnosti informací, zavádění ISMS apod.

2.8 Systém řízení informační bezpečnosti

Informační bezpečnost je v dnešní době již nezbytnou součástí každého informačního systému. Systém řízení informační bezpečnosti (dále jen ISMS) je částí celkového systému řízení procesů v organizaci, jež dokumentuje, implementuje, přezkoumává, udržuje a zlepšuje proces bezpečnosti informací.

[19] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vyd. Brno: Computer Press, 2004. s. 18-19, ISBN 80-251-0106-1.

2.8.1 Rámec ISMS [20]



Obrázek 5: Postup při tvorbě ISMS

Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 52, ISBN 978-80-7251-339-0.

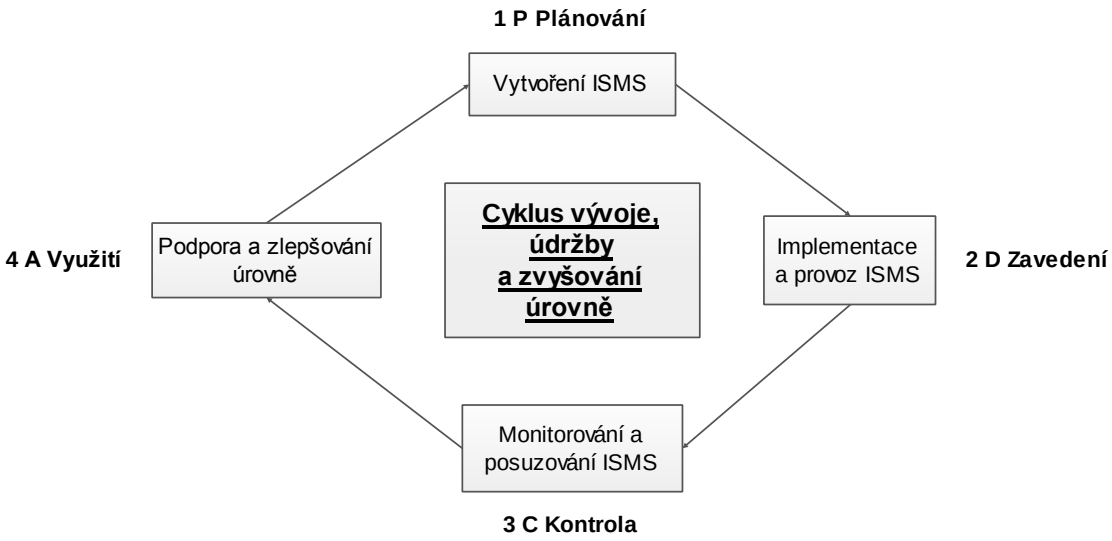
Jak ukazuje obrázek č.5 výše, vývoj ISMS zahrnuje 6 kroků (fází), přičemž fáze 3 a 4 tvoří jádro systému. Jedná se o část zvládání rizik.[21]

[20] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 51-55, ISBN 978-80-7251-339-0.

[21] Rozšiřující informace o řízení rizik lze nalézt v publikaci: Douček, P. – Novák, L. – Svatá, V. – Nedomová, L. *Řízení bezpečnosti informací*. 1. vyd. Professional Publishing, 2008, s. 98-107, ISBN 978-80-86946-88-7.

2.8.2 Závádění ISMS [22]

Systém informační bezpečnosti je možno zavádět podle různých pravidel a předpisů. Nejschůdnější cestou je ale implementovat ISMS podle již definovaného standardu. Tím nejznámněších z nich je mezinárodní norma ISO/IEC 27001. Je to základní norma pro ISMS a představuje osvědčený způsob jak zajistit, řídit, hodnotit bezpečnost informací a integrovat ji do stávajícího systému řízení organizace. Stanovuje požadavky systému řízení na bezpečnost informací a upravuje přístup organizace k řízení rizik a kontrolních cílů a současně i požadovaný stupeň pojištění. Požadavky definované v této normě se blíží reálným potřebám praxe. Závádí se model PDCA sloužící ke stálemu zlepšování ISMS. Model má čtyři kroky a tvoří uzavřený cyklus. Vše je popsáno níže na obrázku č.6.



Obrázek 6: Model PDCA

Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 55-62, ISBN 978-80-7251-339-0.

[22] Kalamár, Š. – Požár, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha : Policejní akademie České republiky v Praze, 2010, s. 55-62, ISBN 978-80-7251-339-0.

2.8.3 Přínosy zavedení ISMS [23]

Přínosy zavedení systému řízení bezpečnosti informací jsou pro organizaci především:

- zefektivnění hlavních procesů organizace,
- zvýšení konkurenční výhody,
- tvorba provozního prostředí zaručujícího bezpečnost informací a ochranu soukromí všech subjektů, jejichž data jsou zpracována,
- snížení rizik nedostupností, úniků či ztráty dat,
- optimalizace nákladů na zajištění bezpečnosti informací vzhledem k hodnotě ochraňovaných aktiv organizace,
- snížení nákladů souvisejících s odstraňováním následků bezpečnostních incidentů,
- snížení nákladů spojených s výpadkem informačního systému organizace a se zajištěním nouzového zpracování dat,
- optimalizace nákladů při obnově chodu informačního systému organizace po jeho výpadku,
- prokázání úsilí o ochraně dat klientů, partnerů, nadřízených orgánů, orgánů státní správy a veřejnosti,
- zvýšení povědomí o bezpečnosti a odpovědnosti zaměstnanců, zvýšení povědomí o bezpečnosti u pracovníků, klientů a případně také u pracovníků třetích stran,
- zlepšení prezentace organizace navenek vůči klientům, vůči partnerům a ostatním organizacím.

[23] Douček, P. – Novák, L. – Svatá, V. – Nedomová, L. *Řízení bezpečnosti informací*. 1. vyd. Professional Publishing, 2008, s. 221, ISBN 978-80-86946-88-7

2.9 Orgány a uskupení ovlivňující oblast informační bezpečnosti

2.9.1 Národní bezpečnostní úřad

Národní bezpečnostní úřad (dále jen "NBÚ") je ústředním orgánem státní správy působícím v oblasti bezpečnostní způsobilosti a v oblasti utajovaných informací. Hlavním úkolem NBÚ bylo připravit návrh zákona o kybernetické bezpečnosti. Celá akce začala věcným záměrem. V Evropě není podobná legislativa trendem. NBÚ má kompetence kontrolovat a napravovat. Měl by být schopen okamžité aktivní reakce a koordinace výjimečného stavu. Stejně tak by měl zprostředkovat certifikaci, akreditaci a zabezpečení standardů kybernetické bezpečnosti.

2.9.2 CERT

CERT je skupina, jež vznikla roku 1988 po aféře s jedním z prvních počítačových červů (tzv. Morrisův červ), který ke svému šíření využíval internet. Od té doby CERT zveřejňuje bezpečnostní rady, zodpovídá přibližně za více než 140 000 zpráv o internetových průlomech. Další činností skupiny je nonstop telefonická podpora. Navíc vydává pravidelné roční zprávy, které poskytují vynikající statistický náhled na danou problematiku.

V roce 2000 bylo skupinou CERT přijato řešení, že bude zveřejňovat varování o zranitelných místech vždy po 45 dnech, a to bez ohledu na to, kde byla objevena. Tím na subjekt vytvoří určitý tlak, aby dané chyby opravil, ale zároveň mu ponechá určitý čas na nápravu.

Informační zprávy skupiny CERT obsahují adresy, na kterých jsou k dispozici opravy s informacemi od daného subjektu. Zde je možné také nalézt nástroje, jejichž pomocí lze zjistit, jak je daný systém proti určité zranitelnosti zabezpečen.

Vládní CERT [24] a týmy typu CSIRT hrají klíčovou roli při ochraně kritické informační infrastruktury.

Každá země, u které existuje propojení kritické informační infrastruktury a internetu, musí být schopna efektivně a účinně čelit bezpečnostním hrozbám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při prevenci. Tyto týmy zároveň působí jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Důležitou roli hrají i při zvyšování vzdělanosti v oblasti bezpečnosti na internetu.

Klíčovým pracovištěm typu CERT v České republice je sdružení CZ.NIC, z.s.p.o. Toto sdružení bylo založeno v roce 1998 předními poskytovateli internetových služeb. V dnešní době má 94 členů a k hlavním činnostem patří provozování registru doménových jmen „.cz“, zabezpečení provozu domény a osvěta v oblasti doménových jmen. Jeho hlavním týmem je CSIRT.CZ. [25]

Od 1. ledna 2011 funguje CSIRT.CZ jako oficiální Národní CERT tým provozovaný sdružením CZ.NIC. CSIRT.CZ tým je zodpovědný za řešení bezpečnostních incidentů na svojí síti a incidentů, které se týkají nameserverů domény „.cz“. Specifikem týmu, správce národní domény, je možnost iniciovat deaktivaci konkrétní domény, z níž pochází bezpečnostní incident národního či mezinárodního významu. Cílem týmu je pomáhat provozovatelům internetových sítí v České republice zřizovat jejich vlastní bezpečnostní týmy a bezpečnostní infrastrukturu, řešit bezpečnostní incidenty a tím zlepšovat bezpečnost jejich sítí i globálního internetu. V rámci své činnosti spolupracuje CSIRT.CZ také se zahraničními subjekty; zejména s nadnárodními organizacemi ENISA, TERENA, a FIRST.

Právě na stránkách CSIRT.CZ týmu můžeme nalézt ty nejaktuálnější statistiky incidentů v kybernetické bezpečnosti. Za zmínku stojí především IDS, který jich za dobu své činnosti od roku 2011 zachytil obrovské množství. Tabulky a grafy se zobrazením počtu incidentů lze nalézt v příloze A a to, jak byly tyto incidenty vyřešeny v příloze B.

[24] Vládní CERT[online]. 2014. Dostupné z WWW: http://www.govcert.cz/cs/vladni-cert/

[25] CSIRT[online]. 2014. Dostupné z WWW: http://csirt.cz/

3 Rozbor návrhu zákona o kybernetické bezpečnosti z hlediska možnosti poskytování bezpečnostních služeb [26]

Národní bezpečnostní úřad dne 28. června 2013 předložil vládě České republiky návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Ve čtvrtek 2. ledna 2014 vláda České republiky schválila návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Návrh zákona bude předložen k dalšímu legislativnímu projednávání v Parlamentu České republiky.

3.1 Hlava I

Hlava I návrhu zákona o kybernetické bezpečnosti se věnuje základním ustanovením. Konkrétně se jedná předmětu úpravy, vymezení pojmů a specifikaci orgánů a osob, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti.

3.1.1 Předmět úpravy

Zákona o kybernetické bezpečnosti upravuje práva a povinnosti fyzických a právnických osob, působnost a pravomoc orgánů veřejné moci a jejich vzájemnou spolupráci v oblasti kybernetické bezpečnosti. Nevztahuje se na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

[26] Tato část práce vychází z informací uvedených v návrhu zákona o kybernetické bezpečnosti, který dne 2.1. schválila vláda České republiky a který bude předložen k dalšímu legislativnímu projednávání.

3.1.2 Orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti

Orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou fyzické nebo právnické osoby (podnikající nebo nepodnikající), na které se vztahuje zákon o kybernetické bezpečnosti. Vyjmenovány jsou v § 3 návrhu zákona o kybernetické bezpečnosti. Tyto osoby musí plnit povinnosti stanovené tímto zákonem, vyhláškami a dalšími právními předpisy od momentu, kdy nastala skutečnost, kvůli které jsou považovány za povinnou osobu.

Za orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti se podle tohoto zákon považují:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud nespadá pod písmeno b),
b) subjekt zajišťující významnou síť, pokud nespadá pod písmeno d),
c) správce informačního systému kritické informační infrastruktury,
d) správce komunikačního systému kritické informační infrastruktury,
e) správce významného informačního systému.

3.2 Hlava II

Hlava II se zabývá systémem k zajištění kybernetické bezpečnosti. Systém zajištění kybernetické bezpečnosti tvoří bezpečnostní opatření, hlášení kybernetických bezpečnostních incidentů, protiopatření, oznamování kontaktních údajů a také činnost Národního bezpečnostního úřadu a dohledových pracovišť (národního CERT).

3.2.1 Bezpečnostní opatření

V § 4 je uvedeno, že bezpečnostní opatření specifikovaná v § 5 jsou orgány a osoby uvedené v § 3 písm. c) až e) přímo povinny zavést pro informační systém kritické informační

infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém a vést o nich důležitou bezpečnostní dokumentaci.

Bezpečnostní opatření jsou v § 5 návrhu zákona rozděleny do 2 skupin, a to na organizační a technická.

Organizační opatření jsou zejména:

- systém řízení bezpečnosti informací,
- řízení rizik,
- bezpečnostní politika,
- organizační bezpečnost,
- stanovení bezpečnostních požadavků pro dodavatele,
- řízení aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
- kontrola a audit kritické informační infrastruktury a významných informačních systémů.

Technická opatření jsou zejména:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců,
- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací,
- bezpečnost průmyslových a řídících systémů.

3.2.2 Detekce a hlášení kybernetických bezpečnostních událostí a incidentů

Detekci a hlášení těchto události a incidentů se věnuje § 7 a § 8 návrhu zákona. Orgány a osoby uvedené v § 3 písm. b) až e) mají povinnost detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému.

Orgány a osoby uvedené v § 3 písm. b) až e) musí hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu.

Orgány a osoby uvedené v § 3 písm. b) jsou povinny hlásit kybernetické bezpečnostní incidenty národnímu dohledovému pracovišti (národnímu CERT).

Orgány a osoby uvedené v § 3 písm. c) až e) hlásí kybernetické bezpečnostní incidenty Národnímu bezpečnostnímu úřadu.

3.2.3 Opatření

Opatřeními se podle § 11 návrhu zákona rozumí úkony Národního bezpečnostního úřadu, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem a nebo k řešení již nastalého kybernetického bezpečnostního incidentu.

Opatřeními jsou:

a) varování (dále rozvedena v § 12),
b) reaktivní opatření (dále rozvedena v § 13),
c) ochranné opatření (dále rozvedena v § 13).

Orgány a osoby, které jsou uvedeny v § 3 jsou povinny bez zbytečného odkladu oznámit NBÚ provedení reaktivního opatření a jeho výsledek. Náležitosti tohoto oznámení stanoví prováděcí právní předpis.

Opatřením obecné povahy stanoví NBÚ orgánům a osobám uvedeným v § 3 písm. c) až e) způsob zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací a lhůtu k jeho provedení. O vydání budou orgány a osoby uvedené v § 3 informovány. Připomínky k opatření obecné povahy lze uplatnit ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce NBÚ.

3.2.4 Kontaktní údaje

Kontaktním údajům orgánů a osob uvedených v § 3 se věnuje § 16 návrhu zákona. Jsou vyžadovány tyto údaje:

a) u právnické osoby obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, adresa sídla, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,
b) u podnikající fyzické osoby obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, adresa místa podnikání a identifikační číslo osoby,
c) u orgánu veřejné moci jeho název, adresa sídla, identifikační číslo osoby (bylo-li přiděleno) a identifikátor orgánu veřejné moci, pokud mu není přiděleno identifikační číslo osoby,
d) údaje o fyzické osobě, která je za povinnou osobu pověřena jednat ve věcech upravených tímto zákonem, v rozsahu jméno, příjmení, telefonní číslo a adresa elektronické pošty.

Kontaktní údaje a jejich změny musí oznamovat:

a) orgány a osoby uvedené v § 3 písm. a) a b) národnímu CERT,
b) orgány a osoby uvedené v § 3 písm. c) až e) NBÚ. Ty oznamují změny pouze těch údajů, které nejsou referenčními údaji vedenými v základních registrech, a to neprodleně.

Vzor oznámení kontaktních údajů a jeho formu stanoví prováděcí právní předpis.

3.3 Hlava V

3.3.1 Správní delikty právnických a podnikajících fyzických osob

Orgány a osoby uvedené v § 3 písm. a) či b) se dopustí správního deliktu tím, že:

a) neprovedou za stavu kybernetického nebezpečí protiopatření vydané NBÚ dle § 13,
b) nesplní některou z povinností uloženou nápravným opatřením dle § 24.

Konkrétní případy, kdy se orgány či osoby dopustí správního deliktu, jsou vypsány v § 25 odstavci 2, výši pokut je věnován odstavec 3. Dále v § 26 je řečeno, že fyzická osoba se dopustí přestupku tím, že poruší povinnost uvedenou v § 10 odst. 1. Za takovýto přestupek se uloží pokuta do 50 000 Kč.

Také následující paragraf (§ 27) se zabývá správními delikty. Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

Odpovědnost právnické osoby za správní delikt zaniká, jestliže NBÚ o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však zaniká do 3 let ode dne, kdy byl správní delikt spáchán.

Při určení výměry pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán.

Pokuta je splatná do 30 dnů ode dne nabytí právní moci rozhodnutí o jejím uložení.

3.4 Hlava VI

3.4.1 Přechodná ustanovení

Jelikož zákon nabude platnosti k 1.1.2015, budou v platnosti přechodná ustanovení. Ta jsou uvedena v § 29 (pro orgány a osoby uvedené v § 3 písm. a) a b)), § 30 (pro orgány a osoby uvedené v § 3 písm. c) a d)) a § 31 (orgány a osoby uvedené v § 3 písm. e)).

4 Praktická část

Praktická část práce obsahuje tři hlavní úseky. Prvním je průzkum trhu, který se zaměřuje převážně na analýzu konkurence. Následuje samotný návrh obchodního modelu a zakončení představuje jeho zhodnocení.

4.1 Průzkum trhu

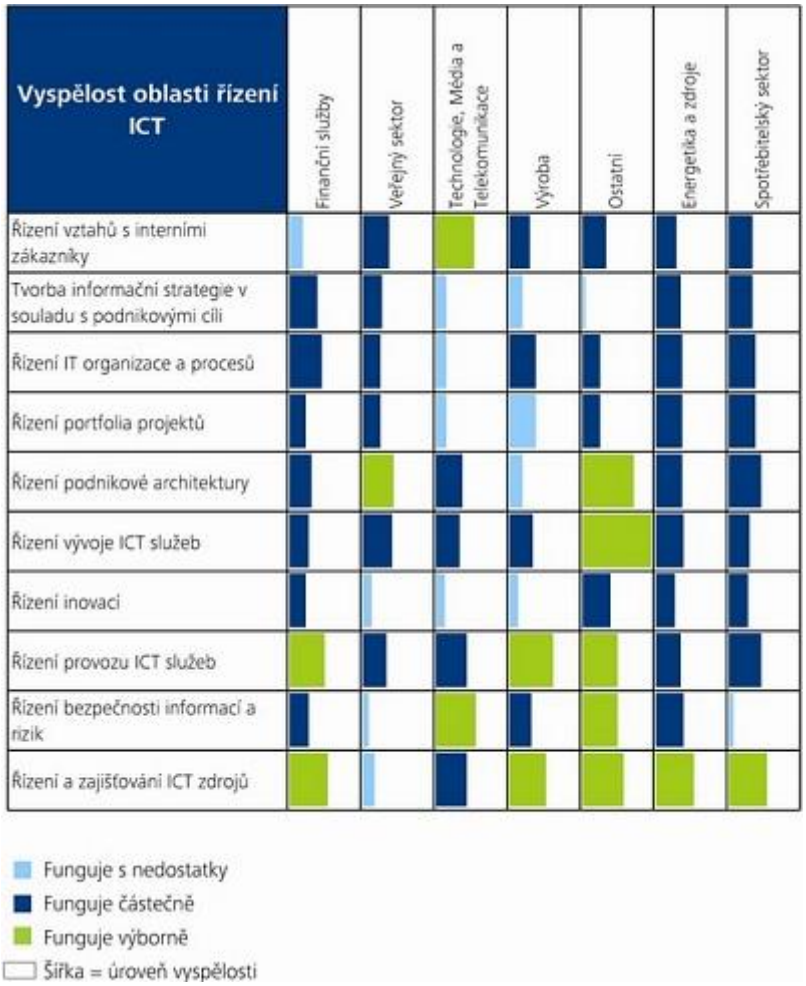
Trh bude velice ovlivněn existencí nového zákona o kybernetické bezpečnosti. Subjekty dotčené tímto zákonem budou totiž povinny zavést bezpečnostní opatření a vést bezpečnostní dokumentaci. Jedná se zejména o řízení rizik, bezpečnostní politiku, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele a bezpečnost lidských zdrojů. Zároveň jsou také vyjmenována technická opatření, která bude nutné zavést. Zde se jedná o fyzickou bezpečnost, ochranu komunikačních sítí, řízení oprávnění přístupu, ochranu před škodlivým kódem, detekci bezpečnostních událostí, kryptografické prostředky a podobně. V této sekci se práce věnuje aktuálnímu stavu informační bezpečnosti a analýze konkurence.

4.1.1 Aktuální stav v oblasti řízení IT a informační bezpečnosti [27]

Průzkum aktuálního stavu v oblasti řízení IT a informační bezpečnosti v České republice byl proveden společností Deloitte na konci roku 2012. Zúčastnilo se ho přes sto respondentů v roli CIO a vedoucích IT manažerů z různých sektorů a zahrnuje odpovědi pracovníků organizací různých velikostí s počtem zaměstnanců menším než sto, ale i organizací, jejichž počet zaměstnanců přesahuje pět tisíc.

[27] SystemOnLine [online]. 2013. Dostupné z WWW: http://www.systemonline.cz/clanky/stav-informacni-bezpecnosti-ocima-ceskych-cio.htm.

Z průzkumu vyplývá, že osm z deseti respondentů považuje řízení informační bezpečnosti a rizik za nejméně vyspělou oblast v jejich firemním IT. Největší prostor pro zlepšení cítí organizace veřejného sektoru, kde sice podle respondentů řízení bezpečnosti funguje, nicméně s velkými nedostatky. Naproti tomu společnosti působící v odvětví technologie, média a telekomunikace značí fungování řízení informační bezpečnosti jako výborné.



Obrázek 7: Vnímání vyspělosti řízení ICT podle jednotlivých oblastí a odvětví

SystemOnLine [online]. 2013. Dostupné z WWW: http://www.systemonline.cz/clanky/stav-informacni-bezpecnosti-ocima-ceskych-cio.htm.

Investice do oblasti řízení informační bezpečnosti by měly růst, narozdíl od let 2008 až 2012, kdy jí byl přikládán stále menší význam. Podle analytiků společnosti Gartner tvoří v EMEA průměrné výdaje na informační bezpečnost 4,2 procenta celkového rozpočtu alokovaného na IT. Podle průzkumu je účelné investování do zvyšování informační

bezpečnosti v očích ICT ředitelů druhým nejvyšším zájmem – v průměru mu přisuzuje vyšší nebo vysokou důležitost čtyřicet procent respondentů.

Největší potenciál pro kybernetickou bezpečnost je v České republice ve spotřebitelském sektoru. Společnosti působící v sektoru energetiky a zdrojů již tento koncept z velké části zavedly nebo aktuálně zavádějí.

4.1.2 Analýza konkurence

Tato část práce se věnuje analýze konkurenčního prostředí, a to konkrétně služeb nabízených třemi společnostmi (Linux, IBM, Annex) a společnostmi nabízejícími certifikaci ISMS podle ISO/IEC 27001.

Linux[28] nabízí řešení v oblasti informačních systémů a zabezpečení. Přestože se zabývá především analýzami, návrhem, dodávkou, instalací, konfigurací a servisem informačních systémů, nabízí také služby v oblasti zajištění kybernetické bezpečnosti dle metodik a standardů národních bezpečnostních autorit zemí EU (NBÚ, BSI), bezpečnostní audity IS, metodiku pro zjištění potřeb a funkčnosti bezpečnostních zařízení IS (firewall, VPN gateway, log collector, IDS/IPS, ticket system).

Provádí také penetrační testy, u kterých je cílem odhalení zranitelností cílového informačního systému, stanovení způsobu jejich možného využití a doporučení vedoucí k jejich nápravě. Tyto penetrační testy rozděluje na dva druhy:

- destruktivní a nedestruktivní,
- externí a interní.

[28] Více informací lze nalézt na: http://www.linuxservices.cz/.

Česká společnost Annex[29] se zabývá dodávkou komplexních služeb v oblasti informačních technologií, zejména pak návrhem a dodávkou systémů pro řešení bezpečných komunikačních sítí a síťového managementu. Kromě toho nabízí i poradenskou a konzultační činnost, školení a technickou podporu v daných oblastech.

Annex NET, s. r. o. je partnerem několika zahraničních výrobců v oblasti hardwaru a softwaru a působí tedy i jako dodavatel/distributor těchto systémů v České republice.

Případem takového partnera je například firma SourceFire, jež se zabývá inteligentním řešením kybernetické bezpečnosti a mění způsob, kterým organizace řídí a minimalizují bezpečnostní rizika ve svých sítích. Řešení společnosti Sourcefire jsou navržena tak, aby na základě procesu Agile Security® byla natolik dynamická, jako je reálný svět, ve kterém jsou nasazena, ať už se jedná o Next-Generation síťová bezpečnostní řešení nebo ochranu proti pokročilému malware.

Dalším příkladem je firma Ipswitch, jež je výrobcem softwaru pro dohled a management datových sítí LAN/WAN a řešení pro bezpečný přenos dat v Internetu. Příkladem mohou být produkty WhatsUp Gold, které monitorují síťovou infrastrukturu i aplikace, mapují sítě, sledují servery, databáze, síťová zařízení, služby a zobrazují jejich výkon.

Možná tu nejrozšířenější a nejkomplexnější nabídku služeb v oblasti kybernetické bezpečnosti nabízí společnost IBM [30]. Jedná se o řadu integrovaných a samostatných řešení založených na odborných znalostech a pokrývajících oblast softwaru a hardwaru.

Pro různá oddělení bezpečnosti má IBM tato řešení:

- správa a zabezpečení podnikových IT zařízení
    - umožnění chytré a rychlé správy IT zařízení a jejich lepší zabezpečení,

[29] Více informací lze nalézt na: http://www.annexnet.cz/.

[30] Více informací lze nalézt na: http://www.ibm.com/cz/cs/.

- ochrana dat
    - zjednodušení procesu šifrování, minimalizace rizika ztráty nebo úniku citlivých dat a zabránění neoprávněnému přístupu k citlivým datům ze strany neautorizovaných zaměstnanců nebo hackerů,
- ochrana infrastruktury
    - zabezpečení firemní sítě, serverů, virtuálních serverů, sálových počítačů a koncových pevných i mobilních stanic. Zahrnuje řešení pro identifikaci, porozumění a blokování vznikajících hrozeb,
- správa identit a řízení přístupu
    - správa přístupových oprávnění a monitorování dodržování předpisů ze strany uživatelů,
- zabezpečení aplikací
    - testování bezpečnosti firemního softwaru a aplikací.

4.1.2.1 Společnosti zabývající se certifikací ISMS

Společností, které kromě EZÚ certifikují ISMS dle ISO/IEC 27001, existuje na našem trhu poměrně velké množství. Za zmínku stojí především společnosti VÚPS [31], EUROCERT [32] a TÜD SÜD [33]. Všechny kladou důraz na bezpečnost informací a její zlepšení po implementaci ISMS. Nabízejí buď certifikaci samotného ISMS nebo certifikaci ISMS v rámci certifikování integrovaného systému, tedy procesu kdy se souběžně ověřuje systém managementu k požadavkům více norem (například ISO/IEC 27001 + ISO 9001).

[31] Více informací lze nalézt na: http://www.vups.cz/4_9_i27001.html.

[32] Více informací lze nalézt na: http://www.eurocert.cz/certifikace/cz/iso-27001.

[33] Více informací lze nalézt na: http://www.tuv-sud.cz/cz-cz.

4.2 Návrh obchodního modelu

4.2.1 Definice obchodního modelu

"The plan implemented by a company to generate revenue and make a profit from operations. The model includes the components and functions of the business, as well as the revenues it generates and the expenses it incurs." [34]

Obchodní model je plán implementovaný společností za účelem generování příjmu a zisku z jejích činností. Zahrnuje nejen komponenty a funkce podnikání společnosti, ale také generované příjmy a vznikající náklady.

Obchodní model představuje podstatu toho, jak firma vytváří a doručuje hodnotu. Zjednodušeně lze říci, že popisuje způsob získávání peněz. Obchodní modely mohou být jednoduché, ale také velmi složité (převážně v případech, kdy existuje více cest, kterými společnost generuje příjem). Musí však vždy vycházet z reálných možností a kapacit podniku. Podnikatel musí znát a měřit účinnost svého obchodního modelu, aby jej mohl průběžně rozvíjet a zkvalitňovat.

4.2.2 Hlavní předpoklady pro formulování strategické vize

- Podle výzkumu společnosti, provedeného společností Deloitte na konci roku 2012, osm z deseti respondentů z řad CIO společností v České republice považuje řízení informační bezpečnosti a rizik za nejméně vyspělou oblast v jejich firemním IT.
- K 1.1.2015 by měl nabýt platnosti nový zákon o kybernetické bezpečnosti, ve kterém jsou v § 3 uvedeny orgány a osoby, kterým se tímto zákonem ukládají povinnosti v oblasti kybernetické bezpečnosti.

[34] Investopedia [online]. 2014. Dostupné z WWW: http://www.investopedia.com/terms/b/businessmodel.asp.

- Záměr společnosti EZÚ proniknout na trh v oblasti kybernetické bezpečnosti.

4.2.3 Obecná vize EZÚ

"*Pro naše obchodní partnery chceme být správnou volbou v oblasti nezávislého ověřování, zkušebnictví a certifikace výrobků a systémů řízení. Prostřednictvím tradičně vysoké odbornosti služeb, inovace, rozvoje klíčových kompetencí a individuálního přístupu jim chceme nabízet takové služby, které naplní a předčí jejich očekávání.*" [35]

4.2.4 Měřitelné cíle pro první rok

Pro první rok bude hlavním hodnotícím parametrem počet obchodních příležitostí a počet zakázek. Při prvním pohledu bude stanoven a následně hodnocen počet obchodních příležitostí společnosti v této oblasti. Při druhém pohledu bude předmětem hodnocení počet zakázek. Pro první rok se počítá se ztrátovostí modelu.

4.2.5 Měřitelné cíle pro horizont 3 let

Pro horizont tří let bude hlavním hodnotícím faktorem parametr financí. Tentokrát se ale bude jednat o kombinaci dvou pohledů, současné stanovení a hodnocení jak cílového obratu společnosti v této oblasti, tak počtu zakázek. K tomu bude navíc hodnocena průměrná cena zakázek.

Dalším cílem bude zisk konkurenční výhody díky inovativnímu přístupu a orientaci na potřeby uživatelů. Pro tento horizont se již musí jednat o model ziskový.

[35] Ezu.cz [online]. 2014. Dostupné z WWW: http://ezu.cz/o-nas/mise-vize-cil/.

4.2.6 Měřitelné cíle pro horizont 5 let

Pro horizont pěti let bude hlavním cílem stanovení a hodnocení podílu na trhu.

Pro horizont pěti let bude zůstávat hodnotícím faktorem i parametr financí. Znovu se bude jednat o současné stanovení a hodnocení jak cílového obratu společnosti v této oblasti, tak počtu zakázek a opět bude navíc hodnocena průměrná cena zakázek.

Dalším cílem bude udržování konkurenční výhody a její neustálé prohlubování, což bude mít vazbu i na již zmíněný podíl na trhu. Zde se ale bude jednat o zisk konkurenční výhody spočívající v rozšíření nabízené hodnoty, nabízení nových služeb. Současně se musí stále jednat o model ziskový.

4.2.7 Nabízená hodnota

V první řadě je důležité zmínit, jaké potřeby zákazníků by měla nabízená hodnota uspokojovat. Hlavní potřebou zákazníků v této oblasti je zajištění funkčního systému bezpečnosti dat. Příčemž u bezpečnosti informací je pro ně důležitá zejména ochrana proti hrozbám, jako je například přerušení, zachycení, modifikace a fabrikace. Další potřebou zákazníků je zajištění průhlednosti a efektivnosti jejich informačních systémů a zaručení návaznosti na požadavky a cíle organizace, které jsou určené vrcholovým vedením organizace.

V návaznosti na potřeby zákazníků lze definovat nabízenou hodnotu, která dané potřeby uspokojuje. Důležitý faktor při tvorbě nabízené hodnoty představuje nástup platnosti nového zákona o kybernetické bezpečnosti, a to k 1.1.2015. Především je to skutečnost, že tento zákon ukládá určitým orgánům a osobám povinnosti v oblasti kybernetické bezpečnosti (viz. § 3 návrhu zákona o kybernetické bezpečnosti).

Nabízené služby se dělí na dva balíčky. Jeden balíček služeb poskytovaný společností EZÚ a druhý poskytovaný její dceřinou společností ELPP. Dělení služeb mezi tyto společnosti

je způsobeno tím, že EZÚ nemůže některé služby z důvodu zachování nestrannosti poskytovat. Grafické zpracování nabízené hodnoty obsahuje příloha C.

Balíček služeb poskytovaných EZÚ:

- CC certifikace – ISO/IEC 15408 [36],
- bezpečnostní testy:
    - rozkrývání datové sítě,
    - odhalování slabin,
    - prolamování hesel,
    - testování bezpečnosti sítí,
    - testování kybernetické bezpečnosti softwaru použitého ve výrobcích,
- certifikace ISMS – ISO/IEC 27001.

Balíček služeb poskytovaných dceřinou společností ELPP:

- školení, technická podpora, konzultační a poradenská činnost v oblasti kybernetické bezpečnosti,
- seznámení s problematikou zákona o kybernetické bezpečnosti a tím, co to bude pro podnik znamenat,
- tvorba a zavádění ISMS odpovídajícího zákonným předpisům, vyhláškám a nařízením ČR a EU a platným technickým normám,
- odborná pomoc a poradenství při tvorbě ISMS v podniku – v souladu s ISO 27002,
- implementace softwaru pro zajištění kybernetické bezpečnosti u výrobků.

4.2.8 Zákaznické segmenty

Zákazníky je třeba rozdělit podle jejich velikosti na tři skupiny:

- Malé podniky - počet zaměstnanců < 100, roční obrat < 30 mil. Kč

[36] Dobře popsanou problematiku CC lze nalézt v publikaci Douček, P. – Novák, L. – Svatá, V. – Nedomová, L. *Řízení bezpečnosti informací*. 1. vyd. Professional Publishing, 2008, s. 73-86, ISBN 978-80-86946-88-7.

- Střední podniky - počet zaměstnanců < 500, roční obrat < 100 mil. Kč
- Velké podniky - počet zaměstnanců > 500, roční obrat > 100 mil. Kč

Toto rozdělení je platné podle standardní metodiky používané v České republice a je nutné hned z několika důvodů. Prvním důvodem je, že většina malých podniků neuvažuje o implementaci ISMS, protože nákladovost realizace je ve většině případů vyšší než ztráty způsobené bezpečnostními incidenty. Zkrátka implementace ISMS pro malé podniky pozbývá smyslu. Naopak u středních a velkých podniků je situace opačná. Zde již ztráty způsobené bezpečnostními incidenty zpravidla převyšují náklady na zavedení ISMS. Druhým důvodem je nový návrh zákona o kybernetické bezpečnosti, ve kterém jsou v jeho § 3 uvedeny orgány a osoby, jimž se ukládají povinnosti v oblasti kybernetické bezpečnosti. V drtivé většině se to opět týká pouze středních a velkých podniků.

Největší příležitost představuje segment středních podniků, pro který je určena jak tvorba a závádění ISMS, tak i následná certifikace a další služby. U velkých podniků se uvažuje především o službě certifikace třetí nezávislou stranou.

Nicméně i malé podniky potřebují zajistit bezpečnost svých informací. Pro malé podniky jsou z balíčků služeb určeny především školení, technická podpora, konzultační a poradenská činnost a bezpečnostní testy.

4.2.9 Zákaznické vztahy

Nejdůležitějšími termíny při budování vztahů jsou:

- důvěra,
- spolupráce,
- sběr dat,
- detailní zjištění potřeb zákazníka,
- návrh optimálního řešení.

Dobré zákaznické vztahy jsou podporovány značkou, logem. Jasná a čitelná značka se lépe pamatuje a asociuje kladné emoce. Nezbytné je pravidelné provádění monitoringu značky.

Nejdůležitějším faktorem v této oblasti je důvěra, nutnost zachování mlčenlivosti o zjištěných datech. Dalším zásadním faktorem je špičková aktivní komunikace. Po vybrání komunikačního kanálu (viz bod 3.2.7) následuje zvolení způsobu komunikace, protože je rozdíl, zda komunikujeme s partnerem či s koncovým zákazníkem. Je dobré dodržovat dvě hlavní zásady:

- být tam, kde jsou zákazníci,
- v různých komunikačních kanálech udržovat odpovídající styl komunikace.

Důležité je využít informace získané monitoringem pro vlastní prospěch. Je vhodné zapracovat na návrzích, stížnostech a připomínkách a svoje produkty či služby neustále vylepšovat.

Jedním z důležitých argumentů pro udržování dobrých zákaznických vztahů je určitě ten, že náklady na získání nového zákazníka bývají zpravidla vyšší než na udržení stávajícího. Zároveň je ale ztracení stávajícího zákazníka zpravidla jednodušší a rychlejší než získání nového.

Při sběru dat je vhodné zaměřit se na následující:

- jména,
- pozice osoby ve firemní struktuře – kdo rozhoduje (on/někdo jiný),
- definování rozsahu pravomocí,
- významná data (narozeniny, svátky, výročí),
- zájmy lidí (koníčky),
- kde nás objevili,
- co nakupují,
- s čím měli problém nebo proč firmu kontaktovali,
- zpětná vazba - co se jim na firmě líbí, co ne, co by chtěli změnit.

Sběr dat se dá provádět mnoha způsoby. Mezi ně patří:

- online dotazníky na našich stránkách,
- placený průzkum,
- e-mailový marketing,
- telefonické oslovování stávajících klientů,
- pořádání soutěží či eventů,
- možnost registrace na webu či do věrnostního programu.

Je nezbytné aby všichni, kteří se zapojí, byli oceněni (minimálně poděkováním). Data jsou vyhodnocována pomocí obsahové analýzy a na základě toho jsou uspořádány všechny navázané kontakty podle různých spojitostí i rozdílností. Dle rozdělení je poté přizpůsoben obsah, nabízené služby a produkty jednotlivým typům zákazníků.

4.2.10 Kanály

Pro neustálé zlepšování komunikační schopnosti podniku je nutné hledání potenciálních prodejních kanálů, cross-selling, up-selling, udržení zákazníka apod.

Mezi vhodné kanály pro komunikaci se zákazníky v této oblasti patří:

- přímý kontakt,
- e-mail,
- telefon/mobil,
- offline komunikace.

Přímý kontakt je pro tuto oblast zdaleka nejlepším a nejdůležitějším kanálem, jelikož jak již bylo řečeno výše, velmi důležitou roli ve vztazích a komunikaci se zákazníky hraje důvěra a nutnost zachování mlčenlivosti o citlivých datech.

4.2.11 Klíčové zdroje

Klíčové zdroje jsou zdroje potřebné pro nabízenou hodnotu, distribuční kanály a zákaznické vztahy. Tyto zdroje jsou rozděleny do oblastí:

- personální zdroje,
- finanční zdroje,
- technické vybavení,
- odborná znalost.

4.2.11.1 Personální zdroje

Jedná se o složení týmu potřebného k poskytování a realizaci nabízené hodnoty. V tomto týmu je řídícím a rozhodujícím článkem odborný manažer produktu. Dále se jedná o skupinu IT specialistů, kteří se věnují provádění bezpečnostních testů, implementaci softwaru pro zajištění kybernetické bezpečnosti u výrobků a technické podpoře pro zákazníky; skupinu auditorů pro certifikaci ISMS podle ISO/IEC 27001 a certifikaci společných kritérií podle ISO/IEC 15408 schopných také poskytování kvalitního školení a poradenské činnosti; odborníky na tvorbu, zavádění a optimalizaci ISMS; člověka s detailní znalostí odpovídajících zákonných norem České republiky a Evropské unie a platných technických norem zastřešujícího oblast školení, technické podpory, konzultační a poradenskou činnost. Zapojení do organizační struktury EZÚ probíhá především přes odborného manažera produktu, dále také auditory, kteří auditují nejen pro tuto oblast. Důležité je především propojení s úsekem obchodu.

4.2.11.2 Finanční zdroje

Zde je nutné rozdělení na dvě fáze alokace financí. V první fázi se jedná o alokaci financí EZÚ pro tento obor a jeho odborný rozvoj, o čemž rozhoduje vrcholové vedení podniku. V druhé fázi se jedná o přidělování financí v rámci obchodní činnosti, což už je úlohou odborného manažera produktu a vedení obchodního úseku.

4.2.11.3 Technické vybavení

Většina činností se obejde bez využití speciálního technického vybavení a bezpečnostních nástrojů, nicméně provádění bezpečnostních testů se již bez podpory automatizovaných nástrojů neobejde. Použití bezpečnostních nástrojů [37]:

- nástroje pro rozkrývání datové sítě - například nmap,
- nástroje pro odhalování slabin - například program NESSUS,
- nástroje pro prolamování hesel - například John the Ripper, který je určen pro prolamování hesel systémů windows a unix,
- nástroje pro testování bezdrátových sítí,
- nástoje pro testování kybernetické bezpečnosti softwaru použitého ve výrobcích.

4.2.11.4 Odborná znalost

Tato oblast vyžaduje hlubokou odbornou znalost. Jelikož se jedná o nový moderní obor, je nutné ji neustále prohlubovat pomocí pokračujícího vzdělávání, účasti na školeních, přednáškách a konferencích. Důležité je také sledování současných změn v odpovídající legislativě, aktualizací technických norem zabývajících se touto problematikou a také světových trendů v oblasti.

4.2.12 Klíčoví partneři

Klíčovým partnerstvím pro tuto oblast je pro EZÚ spolupráce s katedrou telekomunikační techniky elektrotechnické fakulty ČVUT v Praze, která se zabývá kybernetickou bezpečností.

[37] Podrobné informace o nástrojích na provádění bezpečnostních testů a způsobu jejich využití je možné získat např. v dokumentu NIST SP Guidline on Network Security Testing nebo metodice OSSTMM.

Partnerství s dodavateli musí být vždy smluvně zabezpečeno tak, aby bylo zajištěno zachování mlčenlivosti a aby byla udržována vzájemná důvěra, což je v této oblasti nezbytné. Ve většině případů by se jednalo o partnerství se subdodavatelem, tedy fyzickou či právnickou osobou nevystupující ve vztahu k objednateli vlastním jménem a na vlastní odpovědnost. Řešil by se tak nedostatek kapacit EZÚ či ELPP, popř. nižší nákladovost určitých operací při využití subdodavatele a chybějící odbornost v dílčích kategoriích.

4.2.13 Legislativa

Nabízené služby musí odpovídat zákonným normám ČR a EU a platným technickým normám.

V současné době se jedná o již výše zmíněný návrh zákona o kybernetické bezpečnosti. Paragrafové znění návrhu zákona je dostupné veřejnosti od léta 2013 na webových stránkách NBÚ (www.nbu.cz), a to včetně důvodové zprávy. Mezi další zákony patří například zákon č. 106/1999 Sb. o svobodném přístupu k informacím, zákon č. 151/2000 Sb. o telekomunikacích a zákon č.101/2000 Sb. o ochraně osobních údajů.

V případě platných technických norem se jedná o již výše zmíněnou rodinu norem ISO/IEC 27000, z nichž nejdůležitější jsou ISO/IEC 27001 a ISO/IEC 27002. Nicméně tato rodina obsahuje velké množství dalších norem. [38]

[38] Kompletní výčet všech norem rodiny ISO/IEC 27000 dostupný na: http://www.iso27001security.com/html/27000.html.

4.3 Zhodnocení návrhu obchodního modelu

Jelikož se jedná o vytvoření nové nabízené hodnoty, je pro první rok či dva očekávána spíše ztrátovost produktu a od třetího roku se již musí jednat o produkt ziskový. Jedinou částí nabízené hodnoty, která je již společností poskytována, je certikace ISMS podle ISO/IEC 27001.

Ze stejného důvodu neobsahuje návrh obchodního modelu nákladovou strukturu a tok výnosů, protože by se jednalo o čistou a ničím nepodloženou spekulaci s nulovým přínosem. Tento návrh obchodního modelu odráží kapacity a možnosti společnosti EZÚ a její dceřiné společnosti ELPP. Vzhledem k rychlému vývoji a neustálým změnám v této oblasti se očekává i změna a přízpůsobování tohoto modelu v průběhu času současné situaci a požadavkům norem či zákonů. Návrh popisuje všechny služby, které může podnik poskytovat s tím, že v průběhu času dojde k výběru těch, které pro podnik přináší nejvyšší zisk a největší hodnotu pro zákazníky.

Závěr

Cílem této bakalářské práce s názvem *„Návrh obchodního modelu poskytujícího služby v oblasti kybernetické bezpečnosti“* bylo navrhnout obchodní model pro oblast kybernetické bezpečnosti aplikovatelný na společnost EZÚ, jejímž záměrem je kromě poskytování strandartních služeb proniknout také na trh v oblasti kybernetické bezpečnosti.

Začátek práce se věnuje teoretickému zpracování a popsání problematiky, zejména kybernetické bezpečnosti, hrozbám, aplikovatelným normám atd. Poté se začala bakalářská práce věnovat analýze nového návrhu zákona o kybernetické bezpečnosti, kde bylo nejdůležitější popsat skutečnosti, které se týkají osob a orgánů, kterým nový zákon ukládá povinnosti a tyto povinnosti dále popsat. Poslední část práce se již zabývá samotným návrhem obchodního modelu pro oblast kybernetické bezpečnosti. V první řadě byl proveden průzkum trhu, a to včetně analýzy konkurence. Dále následovalo zaměření se na klíčové části obchodního modelu, především na nabízenou hodnotu. Zakončením praktické práce je závěrečné zhodnocení navrženého modelu. Tímto ovšem práce na obchodním modelu nekončí, bude zapotřebí ho nadále upravovat podle možností a sil podniku, podle zpětné vazby od zákazníků a podle jejich potřeb.

Seznam použité literatury

KALAMÁR, Š. - POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. 1. vyd. Praha: Policejní akademie České republiky, 2010. 190 s. ISBN 978-80-7251-339-0.

Douček, P. – Novák, L. – Svatá, V. – Nedomová, L. *Řízení bezpečnosti informací*. 1. vyd. Professional Publishing, 2008, 239 s. ISBN 978-80-7431-079-3.

ANTUŠÁK, E. - KOPECKÝ, Z. *Krizový management - krizová komunikace*. 1. vyd. Praha: Oeconomica, 2005. 92 s. ISBN 80-245-0945-8.

DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

Návrh zákona o kybernetické bezpečnosti [online]. 2014. Dostupné z WWW: www.govcert.cz/download/nodeid-577/.

SystemOnLine [online]. 2013. Dostupné z WWW: http://www.systemonline.cz/clanky/stav-informacni-bezpecnosti-ocima-ceskych-cio.htm.

IBM [online]. 2014. Dostupné z WWW: http://www-01.ibm.com/software/cz/role/security/index.html?CMP=713AH&CT=713AH45W&S_TACT=713AH45W&CR=GOOGLE&CM=K&CCY=CZ&CPB=SWG&CD=2014-02-04&CK=informa%C4%8Dn%C3%AD%20bezpe%C4%8Dnost&CS=QUERY&COT=I&CPG=ILEAD&CO=ON.

Vládní CERT [online]. 2014. Dostupné z WWW: http://www.govcert.cz/cs/vladni-cert/.

ANNEX [online]. 2014. Dostupné z WWW: http://www.annexnet.cz/ o-nas.

CSIRT [online]. 2014. Dostupné z WWW: http://csirt.cz/.

Linux services [online]. 2014. Dostupné z WWW:
http://www.linuxservices.cz/kyberneticka-bezpecnost.

TÜD SÜD [online]. 2014. Dostupné z WWW:
http://www.tuv-sud.cz/cz-cz/cinnosti/audit-a-certifikace-systemu/certifikace-systemu-managementu-bezpecnosti-informaci-dle-iso-27001.

Eurocert [online]. 2014. Dostupné z WWW:
http://www.eurocert.cz/certifikace/cz/iso-27001.

VÚPS [online]. 2014. Dostupné z WWW: http://www.vups.cz/4_9_i27001.html.

Investopedia [online]. 2014. Dostupné z WWW:
http://www.investopedia.com/terms/b/businessmodel.asp.

RobertNemec.com [online]. 2014. Dostupné z WWW:
http://marketing.robertnemec.com/jak-budovat-vztahy-se-zakazniky/.

Novinky [online]. 2013. Dostupné z WWW:
http://www.novinky.cz/internet-a-pc/316722-nejrozsirenejsi-internetove-hrozby.html.

Experiencing Information [online]. 2014. Dostupné z WWW:
http://experiencinginformation.wordpress.com/2011/07/11/business-model-canvas-a-type-of-alignment-diagram/.

CSIRT Incident handling statistics [online]. 2014. Dostupné z WWW:
http://csirt.cz/files/csirt/statistics/stats.html.

Elektronická databáze článků ProQuest:

Masood, M. – Hur, A. – Razzaq, A. – Ahmad, H. F. *Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications*, IEEE Eleventh International Symposium on Autonomous Decentralized Systems, 2013, s. 1-5. ISBN: 978-1-4673-5069-3. Dostupné také z WWW: http://www.computer.org/csdl/proceedings/isads/2013/5069/00/06513420-abs.html.

Patterson, I – Nutaro, J. – Allgood, G. – Kuruganti, T. – Fugate, D. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop.* Článek č. 20, ACM, New York, NY, USA, 2013, s. 1-4. ISBN: 978-1-4503-1687-3. Dostupné také z WWW: http://dl.acm.org/citation.cfm?doid=2459976.2459999.

Mukhopadhyay, A. – Chatterjee, S. – Saha, D. – Mahanti, A. – Sadhukhan, S. K. *Decision Support Systems.* Svazek 56, Elsevier science BV, Amsterdam, Nizozemsko, 2013, s11-26. ISSN**:** 0167-9236. Dostupné také z WWW: http://www.sciencedirect.com/science/article/pii/S0167923613001115.

Seznam příloh

Přílohy

Příloha A Počet incidentů v České republice

Příloha A obsahuje tabulku s počtem incidentů pro každý sledovaný rok (otevřené i uzavřené případy) podle CSIRT.CZ. Uváděné údaje jsou platné za období 1.4.2008 - 6.4.2014.

	2008	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**SUM**
IDS				491	3924	2121	493	7029
Phishing	65	220	209	144	159	175	68	1040
Spam	47	28	103	26	43	73	22	342
Virus		121	178	1	1			301
Malware	53	97	42	9	19	44	15	279
Jiné	1	5	8	62	13	75	20	184
DDoS	1	4	2	2	68	72	11	160
Trojan	66	6	26	5	5	12	11	131
Probe		3	14	25	12	26	29	109
Botnet		3	46	5	8	15		77
Portscan	10	4	1	6	1	3	9	34
Crack	1		4					5
Copyright			1		1			2
Neznámé							1	1
SUM	244	491	634	776	4254	2616	679	9694

Tabulka 1: Počet incidentů pro každý sledovaný rok

Vlastní tvorba

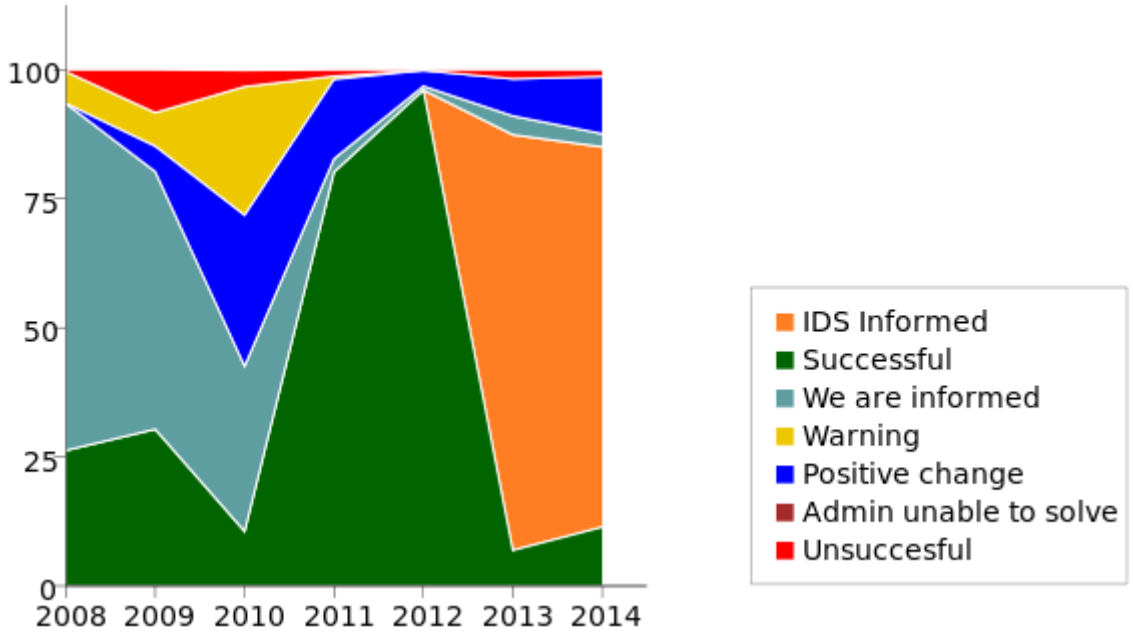
Příloha B Vyhodnocení incidentů v České republice

Příloha B obsahuje tabulku a graf, na kterém lze vidět vyhodnocení incidentů. Zobrazují se v nich pouze uzavřené případy. Uváděné údaje jsou platné za období 1.4.2008 - 6.4.2014.

	2008	2009	2010	2011	2012	2013	2014	SUM
Úspěch	64	149	67	622	4085	180	76	5243
IDS informován						2106	492	2598
Jsme informováni	164	245	203	20	32	95	17	776
Pozitivní změna		24	185	119	130	188	74	720
Varování	15	32	158	5				210
Neúspěch	1	41	20	10	7	47	9	135
Administrátor neschopen řešit			1					1
SUM	244	491	634	776	4254	2616	668	9683

Tabulka 2: Vyhodnocení incidentů pro každý sledovaný rok

Vlastní tvorba

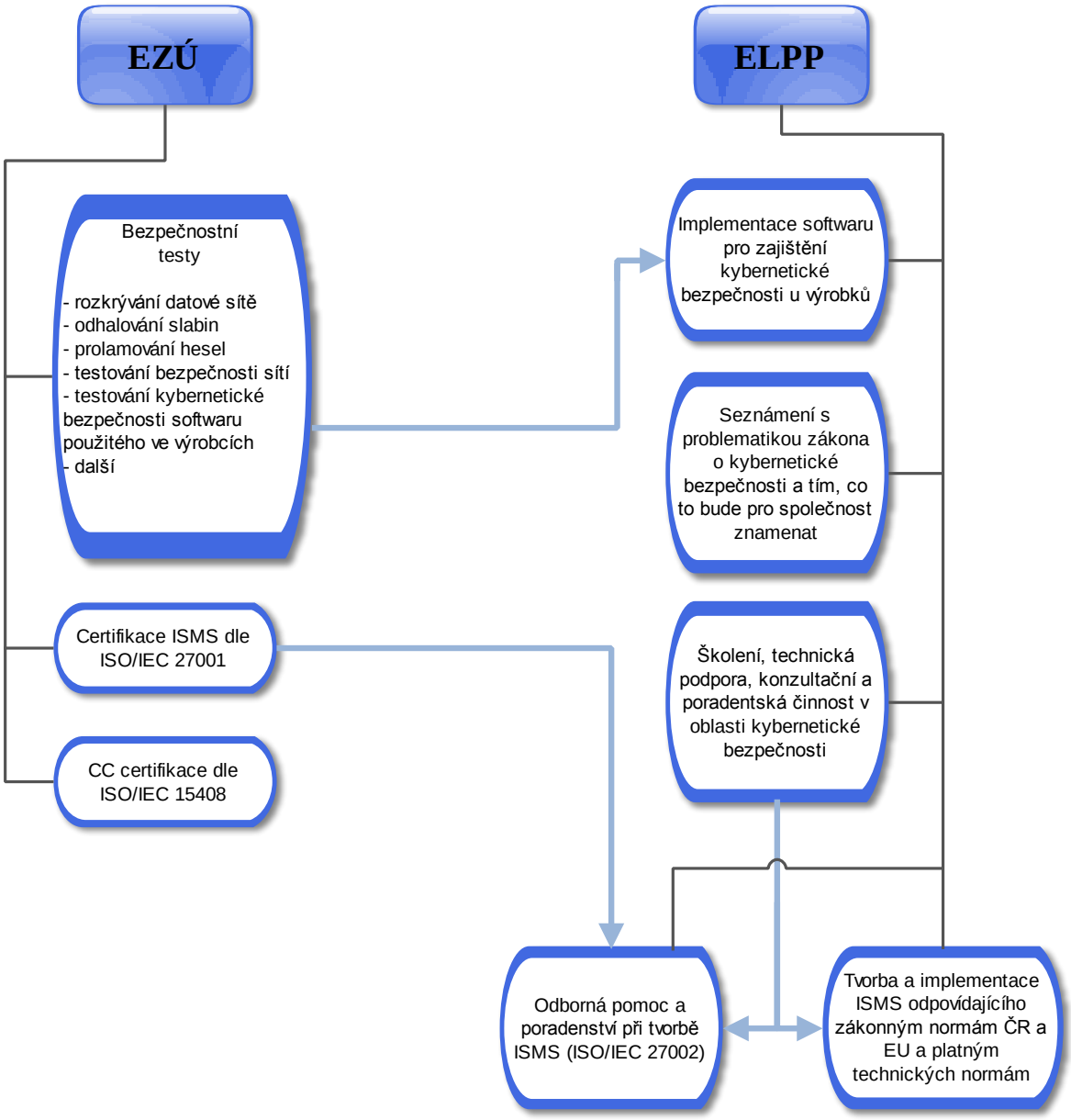


Obrázek 8: Vyhodnocení incidentů za každý sledovaný rok

CSIRT.CZ [online]. 2014. Dostupné z WWW: http://csirt.cz/files/csirt/statistics/stats.html.

Příloha C Schéma nabízené hodnoty návrhu obchodního modelu

Příloha C obsahuje grafické schéma pro sekci nabízené hodnoty návrhu obchodního modelu.

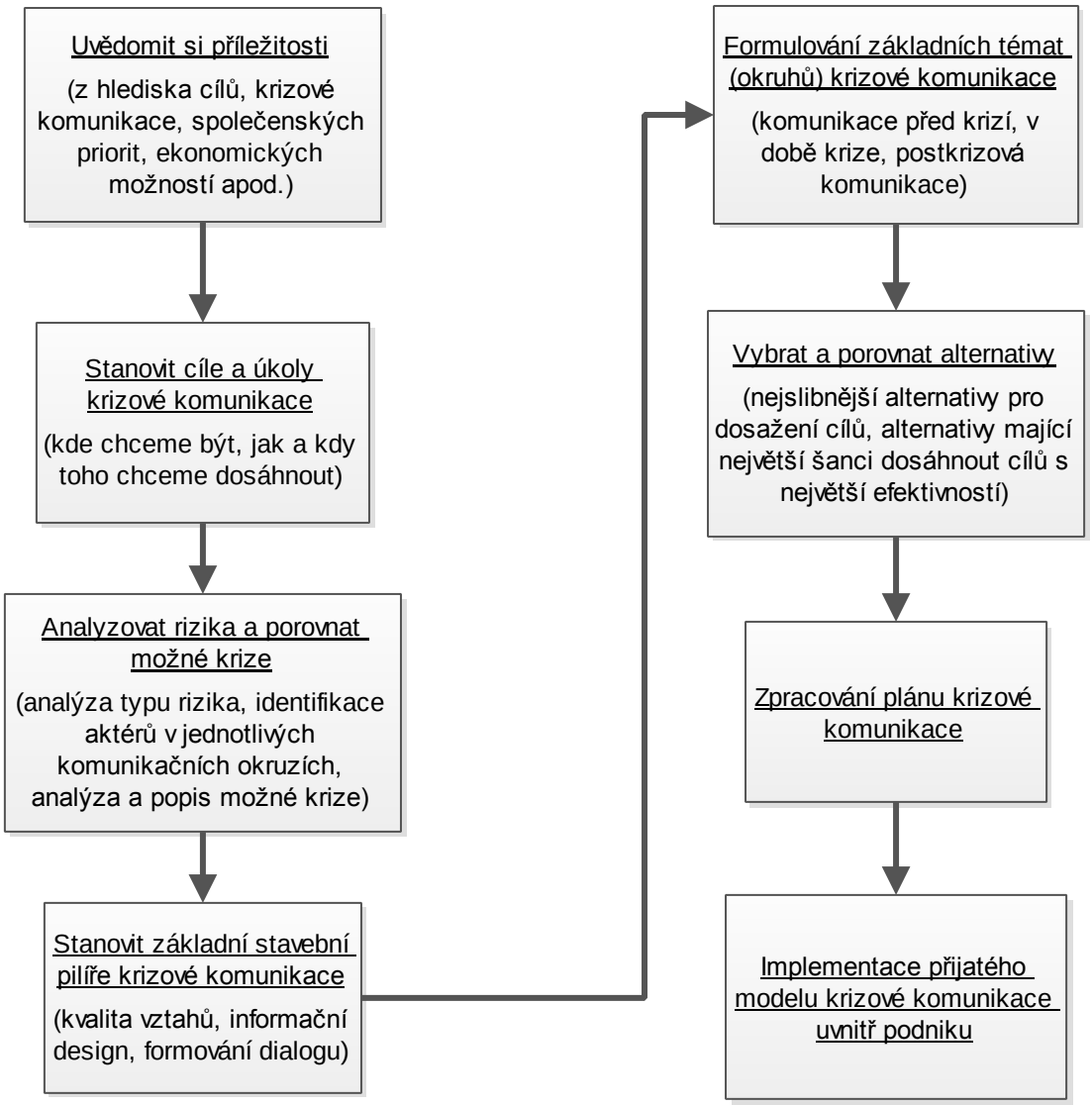


Obrázek 9: Grafické schéma nabízené hodnoty návrhu obchodního modelu

Vlastní tvorba

Příloha D Schéma vytvoření a implementování modelu krizové komunikace uvnitř podniku

Příloha D ukazuje schéma správného průběhu procesu vytvoření a implementování modelu krizové komunikace uvnitř podniku.



Obrázek 4: Schéma vytvoření a implementování modelu krizové komunikace uvnitř podniku

Vlastní tvorba